

Letter to Health Care Financing Administration

October 13, 1998

Health Care Financing Administration
Department of Health and Human Services
Attention: HCFA-0049-P
PO Box 26585
Baltimore, Maryland 21207-0519

(Submitted by E-mail to security@osaspe.dhhs.gov)

Dear Sir or Madam:

This letter provides comments on your August 12, 1998, notice in the Federal Register proposing a rule concerning Security and Electronic Signature Standards. The proposed rule implements security requirements pertaining to the Health Insurance Portability and Accountability Act of 1996.

I am providing these comments as Chair of the Federal Public Key Infrastructure Steering Committee, an organization comprising over fifty representatives from more than two dozen Federal agencies. The Steering Committee promotes the appropriate consideration and use of public key technology for digital signatures and confidentiality (encryption).

We fully support the proposed rule's description of digital signatures as the best available mechanism for ensuring the integrity, nonrepudiation, and authenticity of transactions and data. As a minor item, we note that on page 43273 of the Federal Register notice, the term Asymmetric Encryption is described as meaning that: (1) the key used for encryption is different from the one used for decryption, and (2) neither key can feasibly be derived from the other. The latter statement is not true for all digital signature or confidentiality implementations, for example, those employing the El Gamal rather than RSA algorithm. A more general formulation is that in all digital signature or confidentiality implementations, the private key should not be deducible from the public key.

Separate from but related to the proposed rule, I would like to invite HCFA to provide a representative to the Steering Committee so that you may benefit from the experience and knowledge of representatives from other agencies employing or considering the use of public key technology, and so that we may benefit from your insights and experience as well. The National Institutes of Health of HHS already is represented by Dr. Peter Alterman, but it has been our practice to encourage large departments like HHS, having multiple subordinate agencies, to provide more than one representative where that would be beneficial. That is clearly the case here. Please contact me (Richard.Guida@cio.treas.gov) if you wish to explore this matter.

One of the important initiatives which the Steering Committee has undertaken is the development and implementation of a Bridge Certification Authority (Bridge CA), to facilitate interoperability of CA domains between agencies, and from agencies to external parties. We are currently in the process of developing the Bridge CA and hope to have the design settled and system operational by early 1999. To the extent that HCFA would desire to have any private entity over which you have regulatory authority accept digital certificates issued by HCFA, or that you would desire to accept digital certificates issued by such a private entity or by another Federal agency, the Bridge CA is intended to provide a mechanism which facilitates such interoperability in a scaleable fashion. Participation in the Steering Committee would help ensure that HCFA could stay abreast of our work in this area and make your interests known as we design the Bridge CA and commence operation.

In addition to the Bridge CA, the Steering Committee is also developing guidance addressing, among other things, the proper use of digital signatures for agency applications. This guidance is being prepared by a task force of Steering Committee members from the Social Security Administration, Department of Justice, Department of the Treasury, Office of Management and Budget, and National Partnership for Reinventing Government. We would welcome your appropriate participation in this effort as well.

I appreciate the opportunity to comment on the proposed rule and to supply these additional ideas which will hopefully support your efforts concerning the use of digital signatures. If you have any questions, please contact me at 202-622-1552 or my deputy, Denise Silverberg, at 202-622-1561.

Sincerely,

Richard A. Guida, PE, Chair
Federal PKI Steering Committee